VII kadencja



KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Obrony Narodowej**
(nr 39)
z dnia 3 kwietnia 2013 r.

Pełny zapis przebiegu posiedzenia

Komisji Obrony Narodowej (nr 39)

3 kwietnia 2013 r.

Komisja Obrony Narodowej, obradująca pod przewodnictwem posła **Stefana Niesiołowskiego (PO)**, przewodniczącego Komisji, zrealizowała następujący porządek obrad:

– informacja ministra obrony narodowej na temat bezpieczeństwa teleinformatycznego w siłach zbrojnych;

– informacja ministra obrony narodowej na temat uwzględnienia potrzeb obronności w planowaniu i zagospodarowaniu przestrzennym kraju;

– sprawy bieżące.

W posiedzeniu udział wzięli: **Beata Oczkowicz** i **Waldemar Skrzypczak** podsekretarze stanu w Ministerstwie Obrony Narodowej wraz ze współpracownikami, **Czesław Juźwik** zastępca dyrektora Departamentu Zwierzchnictwa nad Siłami Zbrojnymi Biura Bezpieczeństwa Narodowego oraz **Ryszard Nojszewski** zastępca dyrektora Departamentu Obrony Narodowej Najwyższej Izby Kontroli wraz ze współpracownikami.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Zdzisław Janulewicz, Michał Madaj, Jacek Zientarski** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dzień dobry państwu. Otwieram posiedzenie Komisji. Proszę o zamknięcie drzwi.

Chciałbym bardzo serdecznie powitać panią minister Beatę Oczkowicz, pana ministra Waldemara Skrzypczaka, pana generała Wiesława Orkisza zastępcę szefa Zarządu Planowania Strategicznego Sztabu Generalnego Wojska Polskiego, pana Romualda Hoffmanna dyrektora Departamentu Informatyki i Telekomunikacji MON, pana pułkownika Dariusza Osmulskiego komendanta Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych, pana pułkownika Piotra Wojtona zastępcę szefa Zarządu Dowodzenia i Łączności SGWP, pana Henryka Lewandowskiego dyrektora Biura Inwestycji Specjalnych, pana Czesława Juźwika wicedyrektora Departamentu Zwierzchnictwa nad Siłami zbrojnymi Biura Bezpieczeństwa Narodowego oraz pana Ryszarda Nojszewskiego wicedyrektora Departamentu Obrony Narodowej Najwyższej Izby Kontroli.

Rozumiem, że porządek obrad jest rozdany i jest państwu znany. Czy są uwagi do porządku?

Jeżeli nie ma, traktuję porządek jako przyjęty.

W pierwszym punkcie proszę o zabranie głosu pana generała Waldemara Skrzypczaka.

Podsekretarz stanu w Ministerstwie Obrony Narodowej Waldemar Skrzypczak:

Panie przewodniczący, wysoka Komisjo, problem, który za chwilę przedstawi dyrektor Hoffmann, jest niezwykle istotnym problemem w kontekście bezpieczeństwa systemów zarządzania i kierowania bezpieczeństwem państwa. Ministerstwo Obrony Narodowej podejmuje wiele przedsięwzięć, które zabezpieczają nasze systemy. Incydenty, które się zdarzyły, również w pewnym zakresie dotyczyły Ministerstwa Obrony Narodowej, ponieważ Ministerstwo Obrony Narodowej było obiektem ataków, czyli prób inwigilacji. Szczegóły tego procesu przedstawi dyrektor Departamentu Informatyki i Telekomuni-

kacji pan dyrektor Hoffmann, który zawiaduje komórką realizującą to w Ministerstwie Obrony Narodowej. Czy można panie przewodniczący?

Przewodniczący poseł Stefan Niesiołowski (PO):

Proszę, pan dyrektor Hoffmann.

Podsekretarz stanu w MON Waldemar Skrzypczak:

Proszę bardzo.

Dyrektor Departamentu Informatyki i Telekomunikacji MON Romuald Hoffmann:

Dziękuję. Szanowny panie przewodniczący, wysoka Komisjo, szanowni państwo, w swoim wystąpieniu przybliżę państwu, w jaki sposób budowane są systemy teleinformatyczne w resorcie obrony narodowej. Zaprezentuję podstawowe założenia dotyczące…

Poseł Michał Jach (PiS):

Proszę bliżej mikrofonu.

Dyrektor departamentu w MON Romuald Hoffmann:

To powtórzę jeszcze raz. W swoim wystąpieniu przybliżę państwu, w jaki sposób budowane są systemy teleinformatyczne w resorcie obrony narodowej, zaprezentuję podstawowe założenia dotyczące zapewnienia ich ochrony oraz przedstawię bieżący stan bezpieczeństwa teleinformatycznego w resorcie obrony narodowej.

Określenie stanu bezpieczeństwa teleinformatycznego w resorcie wymaga przede wszystkim zaprezentowania państwu podstawowych zasad przyjętych w resorcie do budowy systemów telekomunikacyjnych. Wiąże się to z tym, że w resorcie obrony narodowej rozwijane są zasadnicze dwa typy systemów teleinformatycznych. Pierwszą grupę stanowią systemy, w których można przetwarzać tylko informacje jawne. Drugą, znacznie ważniejszą dla resortu, grupą są systemy, w których można przetwarzać informacje jawne i niejawne w rozumieniu ustawy o ochronie informacji niejawnych. Chciałbym tutaj przypomnieć, że są to sieci wydzielone. Obie grupy systemów teleinformatycznych tworzą wspólnie umowną wojskową cyberprzestrzeń, za której bezpieczeństwo odpowiada resort obrony narodowej. Ważne jest również to, że te dwie grupy systemów są od siebie odseparowane galwanicznie. Podkreślić należy, że zasadnicza działalność jednostek i instytucji wojska jest prowadzona w systemach drugiej grupy, czyli w takich, w których możemy przetwarzać informacje jawne i niejawne o rocznych klauzulach. Ale nie zapominamy o systemach jawnych.

Systemy przeznaczone tylko do przetwarzania informacji jawnych są to najczęściej systemy dołączone do sieci Internet. Służą one do realizacji zadań publicznych takich, jak obsługa skrzynek pocztowych platformy e-Puap, publikacja Biuletynu Informacji Publicznej, prezentacja ogłoszeń o przetargach publicznych, a także udostępnianie serwisów WWW jednostek i instytucji resortu obrony narodowej. Systemy te służą również, jako uzupełniająca forma komunikacji zewnętrznej resortu obrony narodowej za pomocą poczty elektronicznej jawnej w domenach mon.gov.pl, wp.mil.pl, army.mil.pl, sp.mil.pl i mw.mil.pl. Zasadnicze znaczenie dla funkcjonowania resortu mają systemy należące do drugiej grupy, czyli te, w których możemy przetwarzać również informacje niejawne. Systemy te zgodnie z Ustawą o ochronie informacji niejawnych podlegają dodatkowo nadzorowi ze strony Służby Kontrwywiadu Wojskowego, a poszczególne aspekty związane z ich bezpieczeństwem podlegają szczegółowej kontroli.

W obszarze cyberprzestrzeni, za którą odpowiada resort przy utrzymaniu systemów teleinformatycznych oraz zapewnieniu im bezpieczeństwa prowadzimy zarówno działania techniczne jak również organizacyjne, które są równie ważne. W dalszej części wystąpienia skupię się na sześciu najistotniejszych obszarach wpływających na uzyskany w efekcie poziom bezpieczeństwa systemów teleinformatycznych resortu. Są to: bazowanie na wydzielonych zasobach teleinformatycznych, budowa centrów przetwarzania informacji dysponujących dużą mocą obliczeniową, stosowanie nowoczesnych urządzeń kryptograficznych do ochrony informacji przesyłanych poza strefy ochronne. Jest to również standaryzacja wykorzystywanych narzędzi i ciągły monitoring pracy systemów teleinformatycznych. Jest również współpraca międzyresortowa i międzynarodowa oraz szkolenia specjalistyczne dla administratorów systemów teleinformatycz-

nych. Z tym wiąże się również szkolenie dla personelu posiadającego dostęp do systemów teleinformatycznych resortu obrony narodowej. Każdy z tych obszarów pokrótce omówię.

Zatem przejdę do bazowania na wydzielonych zasobach teleinformatycznych. Wszystkie systemy, w których poza informacjami jawnymi możemy przetwarzać informacje niejawne, budowane są przy wykorzystaniu wydzielonych zasobów telekomunikacyjnych dzierżawionych od operatorów komercyjnych. W chwili obecnej jesteśmy w trakcie budowy na potrzeby resortu obrony narodowej jednolitej warstwy transportowej IP. O skali tego przedsięwzięcia świadczyć może fakt, że jednostki organizacyjne wchodzące w skład sił zbrojnych znajdują się na terenie całego kraju, a także poza jego granicami jak np. kontyngenty wojskowe, ataszaty czy Polskie Przedstawicielstwa Wojskowe przy NATO i UE. Naszym celem jest zapewnienie wysokowydajnego łącza doprowadzonego do każdej lokalizacji, w której funkcjonują nasze jednostki organizacyjne. Jednolita warstwa transportowa, o której wcześniej powiedziałem – nazywamy ją IP – pozwoli nam na skuteczniejsze monitorowanie i przeciwdziałanie pojawiającym się w sieciach zagrożeniom, a także pozwoli nam na optymalizację przydzielania zasobów w zależności od dynamicznie zmieniających się potrzeb sił zbrojnych. Oznacza to, że w przypadku konieczności zapewnienia dużej przepustowości, przepływności łącza na potrzeby systemów krytycznych dla resortu będziemy mogli automatycznie zwiększać przydzielone dla nich zasoby transmisyjne, jednocześnie zmniejszając zasoby przeznaczane dla systemów drugoplanowych. Prostsze i skuteczniejsze będzie również monitorowanie sprawności działania jednolitej warstwy transportowej, niż wielu dedykowanych dla różnych systemów łączy fizycznych.

Budowa centrów przetwarzania jest dla nas niezwykle istotna. Zmiany w warstwie transportowej pozwalają również na dokonanie w tym przypadku skoku jakościowego w zakresie wysokowydajnych punktów przetwarzania i przechowywania informacji, które zapewniają właściwą moc obliczeniową, ale również przestrzeń dyskową do gromadzenia i przetwarzania danych na potrzeby resortu, a one są niemałe. W chwili obecnej realizujemy wiele projektów technicznych, które zaowocują powstaniem kilku takich centrów, zaspokajających bieżące i przyszłe potrzeby resortu. Centralizacja punktów przetwarzania danych wynika przede wszystkim z konieczności zapewnienia ciągłego dostępu do gromadzonych danych. Budowane resortowe centra przetwarzania danych wyposażamy przede wszystkim w odpowiednie, gwarantowane zasilanie. To są dwa kierunki zasilania, z również własnym zasilaniem agregatowym. Zabezpieczamy również bardzo dobre dowiązania transmisyjne, to znaczy łącza o bardzo dużych przepustowościach oraz wysokowydajne systemy klimatyzacji zapewniające odpowiednie warunki pracy. Może nie przy takiej pogodzie, jak teraz, ale latem jest to szczególnie ważne.

Pod względem zapewnienia bezpieczeństwa fizycznego dla przetwarzanych w nich informacji, punkty takie są wyposażone w najnowsze systemy kontroli dostępu, monitorowania ich stanu oraz systemy przeciwpożarowe zabezpieczające nas przed nieuprawnionym fizycznym dostępem do danych lub ich utratą na wypadek np. pożaru. Jako, że rozwiązania stacjonarne są w pierwszej kolejności narażone na oddziaływanie przeciwnika, w projekcie budowy centrów przetwarzania założyliśmy również zakup serwerowni mobilnych, które będą w stanie zabezpieczyć działanie systemów krytycznych dla resortu na wypadek np. zniszczenia serwerowni stacjonarnych. Konsolidacja serwerowni w duże centra przetwarzania i przechowywania danych pozwoli nam na uruchomienie w zasobach resortu prywatnej chmury obliczeniowej. Oznacza to z jednej strony bardzo skuteczne zabezpieczenie danych przed ich utratą, a z drugiej strony umożliwi zapewnienie ciągłego dostępu do danych, ponieważ w przypadku wyłączenia z pracy lub awarii jednej serwerowni, inna serwerownia posiadająca bieżącą kopię zapasową tych samych danych automatycznie przejmie rolę głównej serwerowni dla systemów dotychczas przez nią obsługiwanych.

Do tego żeby praca odbywała się w sposób niezawodny musimy stosować urządzenia kryptograficzne. Z uwagi na to, że dane przetwarzane w resorcie obrony narodowej bardzo często są informacjami niejawnymi w rozumieniu ustawy o ochronie informacji niejawnych, konieczne jest ich zabezpieczenie nie tylko w punktach ich przetwarza-

nia, ale również w trakcie ich przesyłania pomiędzy tymi punktami. Do zapewnienia bezpieczeństwa danych podczas ich transmisji wykorzystujemy urządzenia i narzędzia kryptograficzne, których skuteczność ochrony informacji jest sprawdzana w procesie certyfikacji prowadzonym przez Służbę Kontrwywiadu Wojskowego lub Agencję Bezpieczeństwa Wewnętrznego. W chwili obecnej oczekujemy na zakończenie procesów certyfikacji nowoczesnych, wydajnych urządzeń kryptograficznych zwanych IP Crypto, które pozwolą nam na budowę rozległych systemów teleinformatycznych i ich rozbudowę, w których będzie możliwe przetwarzanie informacji narodowych do klauzuli „Tajne" włącznie w sposób rozległy. Na dalszy wzrost bezpieczeństwa i zwiększenie efektywności pracy urządzeń kryptograficznych pozwolą projektowane i budowane elektroniczne systemy zarządzania danymi kryptograficznymi na potrzeby systemów kryptograficznych NATO, jak i innych sojuszów. Uruchomienie tych systemów zwiększy szybkość wymiany kluczy kryptograficznych i znacząco uprości proces dystrybucji materiałów kryptograficznych na potrzeby funkcjonujących systemów ochrony kryptograficznej. W chwili obecnej w resorcie trwają również prace nad uruchomieniem, wspólnie z Agencją Bezpieczeństwa Wewnętrznego, Narodowego Centrum Kryptologii, którego głównym zadaniem będzie opracowanie algorytmów kryptograficznych na potrzeby sił zbrojnych Rzeczypospolitej Polskiej i nie tylko.

Standaryzacja wykorzystywanych narzędzi i ciągły monitoring pracy systemów teleinformatycznych jest przedsięwzięciem złożonym. W roku ubiegłym resort obrony narodowej podpisał z firma Microsoft umowę Enterprise Agreement zapewniającą zarówno dostawę oprogramowania systemowego, jak i biurowego, na potrzeby systemów teleinformatycznych przetwarzających informacje niejawne, jak i usługę wsparcia technicznego dla zakupionego oprogramowania. Wspomnę tutaj, że resort obrony w większości wykorzystuje oprogramowanie firmy Microsoft. Stąd też podpisano to porozumienie. Poza czynnikami ekonomicznymi przemawiającymi za podpisaniem tego typu umowy, równie ważna dla nas jest możliwość uzyskania specjalistycznego wsparcia technicznego ze strony firmy Microsoft. Poza samą umową, o której wspomniałem – Enterprise Agreement – resort przystąpił również do programu bezpieczeństwa firmy Microsoft zwanego Security Cooperation Program. Celem tego programu jest współpraca pomiędzy instytucjami rządowymi i firmą Microsoft w obszarze bezpieczeństwa teleinformatycznego. Jest ona realizowana poprzez wymianę informacji i realizację wspólnych przedsięwzięć w tym obszarze. Dzięki temu uzyskaliśmy m.in. dostęp do baz wiedzy firmy Microsoft z zakresu bezpieczeństwa teleinformatycznego, a także otrzymujemy informacje o wykrytych nowych podatnościach produktów firmy Microsoft jeszcze przed ich oficjalna publikacją.

Rozległe systemy teleinformatyczne, jakie posiadamy w resorcie, które przetwarzają informacje niejawne, objęte są pełnym monitoringiem pracy i centralną ochroną antywirusową, pozwalającą nam na zminimalizowanie prawdopodobieństwa infekcji systemów za pomocą kodów złośliwych. Centralne zarządzanie ochroną antywirusową pozwala nam na zapewnienie odpowiedniej aktualizacji baz danych oprogramowania niepożądanego w każdej stacji roboczej funkcjonującej w systemie, a także umożliwia nam bezpośrednią reakcję na pojawiające się zagrożenia. Systemami ochrony antywirusowej zarządza wyspecjalizowana komórka MIL-CERT, wchodząca w skład Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych, nadzorowana przez System Reagowania na Incydenty Komputerowe. Jest to struktura, która istnieje w resorcie obrony narodowej od 2008 r. Jest ze mną również pan płk Osmulski, który jest komendantem rzeczonego Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych.

W roku ubiegłym System Reagowania na Incydenty Komputerowe – tutaj odniosę się do systemów jawnych – obsłużył około 4900 różnego typu incydentów komputerowych, mierzonych w dziesięciu kategoriach incydentów. Wspomnę tutaj, że 63% to wykryte oprogramowanie złośliwe na nośniku zewnętrznym, takim jak pendrive, z czego 4% to infekcja stacji roboczej w wyniku tego, a 33% to brak aktualizacji systemu operacyjnego. Wynika to z różnych przyczyn. Ponieważ większość incydentów związanych była z kodem złośliwym pochodzącym z nośników zewnętrznych, dlatego też na początku

2012 r. dla systemów niejawnych wdrożyliśmy system kontroli dostępu do nośników dołączanych do portów USB. Wdrażanie systemu w wyraźny sposób ograniczyło liczbę incydentów tego typu występujących w sieci Internet, ale również ograniczyło zdarzenia, do których dochodziło w sieciach niejawnych.

Dużą wagę resort przywiązuje do współpracy międzyresortowej i międzynarodowej. Wspomnę tutaj, że w ramach współpracy międzynarodowej już w 2010 r. resort podpisał umowę z Departamentem Obrony Stanów Zjednoczonych regulującą zasady wymiany informacji o zagrożeniach w sieciach oraz współpracy w zakresie bezpieczeństwa informacji. Umowa ta pozwoliła nam na realizację wymiany doświadczeń i zdobycie nowej wiedzy, a także znacznie zwiększyła możliwości szybkiego reagowania na nowe zagrożenia. Bardzo duże znaczenie, szczególnie dla zapewnienia bezpieczeństwa systemów dołączonych do sieci Internet, przywiązujemy do współpracy z Agencją Bezpieczeństwa Wewnętrznego, która w tym obszarze realizuje zadania obrony cyberprzestrzeni Rzeczypospolitej Polskiej w obszarze cywilnym. W roku ubiegłym resort obrony narodowej, minister obrony narodowej podpisał z szefem Agencji Bezpieczeństwa Wnętrznego porozumienie w sprawie współpracy w zakresie Systemu Reagowania na Incydenty Komputerowe, gdzie została określona ścisła współpraca w tym zakresie. Personel Systemu Reagowania na Incydenty Komputerowe podnosi swoje kompetencje również w ramach szkoleń i ćwiczeń krajowych i międzynarodowych. Podam tylko kilka z nich. Były to m. in. ćwiczenia: CYBER-EXE, CIWX, Cyber Endeavour i NATO CMX.

Szkolenie personelu posiadającego dostęp do systemów teleinformatycznych resortu obrony narodowej realizowane jest w sposób ciągły. Ponieważ występowanie incydentów komputerowych związane jest w wielu przypadkach z niewłaściwym działaniem użytkowników systemów teleinformatycznych, personel Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych prowadzi ciągłe szkolenia profilaktyczne z zakresu bezpieczeństwa teleinformatycznego na rzecz instytucji i jednostek Resortu obrony narodowej. Z uwagi na wdrażane ciągle nowe technologie i pojawiające się w związku z tym nowe typy zagrożeń, takie szkolenia prowadzone są w trybie ciągłym. Szkolenia te wspierane są dystrybucją za pomocą poczty elektronicznej wewnętrznych biuletynów bezpieczeństwa, w których prezentowane są najnowsze informacje z zakresu bezpieczeństwa teleinformatycznego i – jak to nazywamy – tzw. higieny komputerowej, czyli dobrych praktyk w obszarze użytkowania w sposób bezpieczny systemów IT.

Szanowny panie przewodniczący, wysoka Komisjo, przejdę w tej chwili do oceny bieżącego stanu bezpieczeństwa teleinformatycznego, po czym zakończę wnioskami. W chwili obecnej największe zagrożenie dla bezpieczeństwa informacji identyfikujemy w systemach jawnych dołączonych do sieci Internet. Ochrona tych zasobów jest istotna przede wszystkim z punktu widzenia zachowania właściwego wizerunku, ale i stałej pracy Ministerstwa Obrony Narodowej. Z uwagi na występowanie bezpośredniego połączenia pomiędzy tymi systemami a Internetem naturalne jest to, że są one najbardziej narażone na działania niepożądane. Z tego względu infrastrukturę Ministerstwa Obrony Narodowej centralizującą dostęp do Internetu włączono do programu ARAKIS-GOV, co pozwoliło na detekcję nowych zagrożeń w sieci InterMON, również tych niewykrywalnych za pomocą klasycznych systemów bezpieczeństwa. Zakupiono i wdrożono system wykrywania i przeciwdziałania włamaniom w sieci do monitorowania w trybie ciągłym ruchu sieciowego w punktach styku sieci InterMON z siecią Internet, z równoczesną możliwością blokowania wykrytych ataków sieciowych oraz ruchu niepożądanego. W celu podniesienia poziomu bezpieczeństwa zasobów resortu udostępnianych w sieci Internet podjęto decyzję o przeniesieniu wszystkich zasobów informacyjnych resortu umieszczonych na serwerach różnych jednostek i firm na zasoby własne resortu zarządzane centralnie.

Reasumując, w chwili obecnej stan bezpieczeństwa teleinformatycznego w resorcie obrony narodowej oceniam jako dobry. Realizowane projekty bez wątpienia pozytywnie wpływają i wpłyną na stan zapewnienia bezpieczeństwa teleinformatycznego w resorcie obrony narodowej. Dzięki odpowiedniemu poziomowi finansowania zadań w tym obszarze nie widzę zagrożeń dla realizacji projektów.

Ale co w przyszłości? Nasuwają się następujące wnioski. W najbliższych latach czeka nas wiele zadań związanych z dalszą rozbudową infrastruktury i systemów teleinformatycznych na potrzeby eksploatowanych i budowanych systemów informatycznych i zautomatyzowanych systemów dowodzenia sił zbrojnych. Przykładem takiego wyzwania jest wdrażanie Wieloszczeblowego Systemu Informatycznego resortu obrony narodowej, którego podstawowym zadaniem jest zinformatyzowanie i zintegrowanie obszaru kadr, logistyki i finansów w skali całego resortu. Zapewnienie bezpieczeństwa tych zasobów przy jednoczesnym zagwarantowaniu ciągłości dostępu do danych z każdej jednostki organizacyjnej resortu jest dla nas dużym wyzwaniem, zarówno technologicznym jak i organizacyjnym. Pamiętać trzeba, że rozbudowa systemów informatycznych wiąże się ze wzrostem liczby użytkowników systemów, którzy – jak jasno wskazują nasze statystyki – są właśnie największym – przykro to powiedzieć – zagrożeniem dla bezpieczeństwa tych systemów. Większość z obsługiwanych przez nasze służby techniczne incydentów, to incydenty związane z niewłaściwym postępowaniem użytkowników.

Po uruchomieniu w bieżącym roku centrów przetwarzania danych oraz w przyszłości duży nacisk będziemy kłaść na znowelizowanie procedur odtwarzania sprawności systemów po ich całkowitej awarii z uwagi na zmiany w architekturze technicznej systemów. Zakładamy również uruchomienie w bieżącym roku wewnętrznie w resorcie podpisu elektronicznego i rozpoczęcie procesu wdrażania na jego bazie mechanizmów silnego uwierzytelniania oraz kontroli dostępu do resortowych systemów teleinformatycznych. Chodzi tu przede wszystkim o systemy niejawne.

W obszarze współpracy krajowej i międzynarodowej chcemy wypracować skoordynowane mechanizmy wymiany informacji z narodowymi zespołami reagowania na incydenty komputerowe oraz utrzymać na stałym poziomie dotychczasową współpracę ze strukturami NATO, jak i z zespołami sojuszniczymi. Nadal jednak jednym z najistotniejszych czynników wpływających na bezpieczeństwo teleinformatyczne resortu będzie posiadanie wysoko wykwalifikowanych kadr IT. Pomimo korzystniejszej oferty finansowej firm komercyjnych jestem przekonany, że ciekawa, pełna wyzwań praca w zespołach wdrażających najnowocześniejsze rozwiązania technologiczne oraz szeroki wachlarz oferowanych szkoleń specjalistycznych pozwolą nam na zapewnienie niezbędnego wzrostu naszych zasobów kadrowych w obszarze IT, co z pewnością przełoży się na zwiększenie bezpieczeństwa teleinformatycznego.

Dziękuję panie przewodniczący.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Proszę państwa, jak państwo wolicie? Czy w tej chwili chcą państwo wysłuchać w drugim punkcie informację o obronności i przeprowadzić łączną dyskusję, czy teraz przeprowadzić dyskusję, a potem wysłuchać drugie wystąpienie? Proszę? Czyli teraz dyskusję? Proszę bardzo. Otwieram dyskusję. Pani posłanka Butryn.

Poseł Renata Butryn (PO):

Dziękuję panie przewodniczący. Z dużym zainteresowaniem przeczytaliśmy przedstawione tu wcześniej materiały i wysłuchaliśmy wypowiedzi i pana uwag dotyczących przede wszystkim rozbudowy systemu teleinformatycznego. Zapowiada się to bardzo imponująco, nawet w kontekście naszych sojuszy, bo o tym również trzeba mówić, że coraz bardziej trzeba będzie patrzeć na rozwój teleinformatyczny w kontekście NATO i w kontekście sojuszy europejskich.

W czasie pobytu w Estonii, do którego ciągle powracam, podnoszony był temat bezpieczeństwa w cyberprzestrzeni, ponieważ Estonia jest państwem, które jest e-państwem i e-społeczeństwem i właściwie przeżyła takie dwa ataki cybernetyczne. Zwróciliśmy wraz z posłami uwagę na to, co nazywa się właśnie rozbudową bezpieczeństwa. W Estonii powstał specjalny departament, który ma miejsce szczególne w zakresie obronności kraju i w zakresie ochrony e-społeczeństwa przed tego typu atakami. Ten departament jest ciągle rozbudowywany. Jak gdyby nawet wyprzedza to, co się wprowadza w zakresie informatyzacji społeczeństwa. Bardzo ciekawym elementem pracy tego departamentu jest prowadzenie ćwiczeń. Te ćwiczenia są bardzo częste. Ćwiczenia polegają na markowaniu takiego ataku w cyberprzestrzeni. Chciałabym zapytać, czy resort przewiduje tego

typu ćwiczenia na bardzo wysokim poziomie, żeby w ten sposób sprawdzać już istniejący system i myśleć o zabezpieczeniu tego, co zamierzamy wprowadzać? Dziękuję bardzo.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Pani posłanka Zakrzewska.

Poseł Jadwiga Zakrzewska (PO):

Ja?

Przewodniczący poseł Stefan Niesiołowski (PO):

Zapisała się, nie? Jeśli nie, to przepraszam.

Poseł Jadwiga Zakrzewska (PO):

Ja chciałam zwrócić uwagę na to, czy resort w ogóle przeprowadza analizę ryzyka w odniesieniu do infrastruktury sieci oraz wszystkich elementów i urządzeń? Chciałam też zwrócić uwagę na bezpieczeństwo personalne. Otóż w sieci znalazłam ofertę człowieka, który pracował w Dowództwie Wojsk Lądowych. Był na stanowisku informatyka w pracowni, czy sekcji obrony narodowej. Teraz pracuje w spółce i poszukuje kontaktów biznesowych. Jak resort jest przygotowany do tego, żeby informacje, które uzyskał w Ministerstwie Obrony Narodowej nie zostały wykorzystane w biznesie, czy w innych dziedzinach?

Pan dyrektor Hoffmann powiedział, że w obszarze współpracy krajowej i międzynarodowej zamierza się wypracować skoordynowane mechanizmy wymiany informacji z narodowymi zespołami reagowania. Jakie działania prowadzi Ministerstwo Obrony Narodowej w tym zakresie i dlaczego tak późno? Dziękuję.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję. I trzeci głos. Pan poseł Kamiński. Potem odpowiedź i kolejne pytania. Proszę.

Poseł Mariusz Antoni Kamiński (PiS):

Dwa krótkie pytania. Pierwsze. Jak resort poradził sobie z tymi atakami podczas protestów w sprawie ACTA, kiedy praktycznie serwery wszystkich ministerstw zostały zaatakowane przez hakerów? Jak wtedy na tym tle wypadł resort obrony narodowej?

I drugie pytanie. Jak wygląda kwestia wymiany informacji elektronicznej z ataszatami wojskowymi? Czy to jest korzystanie z tych sieci, które ma Ministerstwo Spraw Zagranicznych, bo np. wszystkie placówki, wszystkie ambasady są podpięte pod MSZ? Czy podobnie jest z ataszatami? Czy jest to przez Ministerstwo Obrony Narodowej, czy przez Ministerstwo Spraw Zagranicznych?

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Chciałbym przeprosić pana posła Jacha, bo pan był w kolejności, ale ja źle zrozumiałem. Pani przewodnicząca powiedziała „Jach", a ja zrozumiałem „ja". Oczywiście teraz, po tych odpowiedziach panów z Ministerstwa pierwszy będzie pan poseł Jach. Jeszcze raz bardzo przepraszam. Proszę bardzo.

Poseł Michał Jach (PiS):

Dziękuję panie przewodniczący. Aha, po odpowiedziach. Dziękuję.

Podsekretarz stanu w MON Waldemar Skrzypczak:

Panie przewodniczący, wysoka Komisjo, w odpowiedzi na pytanie pani poseł Butryn, zgodnie z decyzją ministra obrony narodowej pan generał Bondaryk powołany został na pełnomocnika ministra obrony narodowej m.in. do spraw budowy Narodowego Centrum Kryptografii. W naszych działaniach Ministerstwo Obrony Narodowej nadaje temu problemowi wysoką rangę, po incydentach, które były dużo wcześniej, a które wcześniej nie dotyczyły Ministerstwa Obrony Narodowej. Na bieżąco prowadzi się ocenę zagrożeń, które występują w sieci. Mamy centrum monitoringu, które przez cały czas, na bieżąco monitoruje sieć. Możemy we właściwy sposób reagować.

Ćwiczenia są prowadzone w ramach ćwiczeń z wojskami. Są takie elementy, czy epizody ćwiczeń, w których prowadzi się takie sytuacje. Trzeba jednak mieć świadomość jednej rzeczy, a mianowicie to personel decyduje o wszystkim, o tym, jak reaguje na ataki i zagrożenia w Internecie. Doświadczenia ostatnich tygodni dobitnie świadczą o tym,

że to nie systemy zawiodły, ale ludzie zawiedli. Główny nacisk w tej chwili kładziemy na przygotowanie personelu, który ma właściwie obsługiwać te narzędzia, którymi się posługuje.

Jeśli chodzi o odpowiedź na pytanie pani poseł Zakrzewskiej, to ocenę ryzyka prowadzi się na bieżąco. W zasadzie prowadzi się ją na wszystkich szczeblach dowodzenia. U pana dyrektora Hoffmanna jest centrum, które te zagrożenia na bieżąco analizuje. Dlatego też, jak pani była uprzejma zauważyć, to ludzie decydują o tym, jak to wszystko chodzi. W związku z tym ci ludzie są objęci permanentnym szkoleniem. Ja mam świadomość tego, że chyba niedostatecznym chyba warto wrócić do tego, co powiedziała pani poseł Butryn. U nas jeszcze nie docenia się tego zagrożenia, jakie może powstać w cyberprzestrzeni poprzez tego typu działania, jakie zdarzyły się ostatnio. Myślę, że o szczegółach tego, jak się zabezpieczamy, powie pan dyrektor Hoffmann. Proszę.

Przewodniczący poseł Stefan Niesiołowski (PO):

Pan dyrektor.

Dyrektor departamentu w MON Romuald Hoffmann:

Dziękuję panie przewodniczący. Panie przewodniczący, wysoka Komisjo, będę odpowiadała na pytania w kolejności, w jakiej były zadane.

Podsekretarz stanu w MON Waldemar Skrzypczak:

Ale krótko.

Dyrektor departamentu w MON Romuald Hoffmann:

Krótko. Oczywiście, ćwiczenia przewidujemy. Uczestniczymy w nich. Jak powiedział pan minister Skrzypczak, mamy zarówno ćwiczenia wewnątrz sił zbrojnych, jak również bierzemy udział w ćwiczeniach międzynarodowych. Podam tylko, że w 2012 r. braliśmy udział w takich ćwiczeniach międzynarodowych, w których prowadziło się działania typu obrona, odpowiedź, a mianowicie w ramach ćwiczeń CIWX w czerwcu ubiegłego roku, w ramach „Cyber Endeavour" we wrześniu 2012 r. w Niemczech. Partnerzy są zapraszani m.in. na ćwiczenia do Stanów Zjednoczonych. Braliśmy tam udział jako kluczowy komponent obrony cyberprzestrzeni. Ćwiczenia NATO CMX, które odbyły się w listopadzie ubiegłego roku, dotyczyły m.in. infrastruktury krytycznej, gdzie tego typu rzeczy były również ćwiczone. Wspomnę również o ćwiczeniach, które były realizowane w kraju. Były to np. ćwiczenia CYBER-EXE realizowane przez część cywilną, nie wojskową, a my wzięliśmy w nich udział, jako ludzie w mundurach. Mam nadzieję, że pokrótce odpowiedziałem na pytanie zadane przez panią poseł Butryn.

Uzupełniając wypowiedź pana ministra, jeśli chodzi o analizę ryzyka, to oczywiście prowadzimy to. Robimy to na bieżąco. Mamy służby, które pracują 24 godziny na dobę 7 dni w tygodniu. Pracują na zmiany. Mają odpowiednie narzędzia informatyczne, które pozwalają na aktualną ocenę w sieci jawnej, tej dołączonej do Internetu, jak i w sieciach niejawnych. System monitoringu działa ciągle w ramach systemu reagowania na incydenty komputerowe, bo tak to określamy. Zatem to ryzyko jest za każdym razem określane. Poza tym są cotygodniowe meldunki w tym zakresie. Jako, że jestem odpowiedzialny w resorcie za ten zakres działania, w związku z tym mam na bieżąco informację o tym, jaki mamy poziom bezpieczeństwa w sieciach jawnych i niejawnych.

Współpracujemy od dłuższego czasu ze środowiskiem cywilnym. Współpracujemy od zarania powstania systemu reagowania na incydenty komputerowe. Przy okazji jesteśmy członkiem nieformalnego stowarzyszenia, jakim jest „Abuse". Natomiast to, co miałem na myśli mówiąc „skoordynowane" znaczy, że trzeba byłoby sformalizować niektóre elementy współpracy. Wymaga to określenia zarówno obowiązków, jak i praw z obu stron tak, żeby każda strona mogła wiedzieć, na co może liczyć i w jakim zakresie powinniśmy się poruszać. Jeżeli pani poseł pozwoli, to na tym zakończę odpowiedź na to pytanie.

Przeszedłbym…

Podsekretarz stanu w MON Waldemar Skrzypczak:

Przepraszam, może jeszcze chwilę. Panie przewodniczący, wysoka Komisjo, pani poseł, jeżeli to był żołnierz, który ogłasza się i szuka kontaktów, to ten żołnierz jest związany przysięgą wojskową, którą składał. W zasadzie aż do śmierci powinien przestrzegać tego,

co przysięgał, w związku z tym nie może ujawniać informacji, które są informacjami od zastrzeżonych wzwyż. Jeżeli był to pracownik wojska, to podpisał zobowiązanie, że przez okres 3 lat będzie przestrzegał tajemnicy wojskowej i powinien tej tajemnicy przestrzegać. Jeżeli on ujawnia jakiekolwiek informacje w Internecie i jest to niezgodne z prawem, czyli np. ujawnia tajemnicę wojskową lub służbową, to będzie ścigany przez właściwe organy.

Dyrektor departamentu w MON Romuald Hoffmann:

Jeżeli mogę uzupełnić, to takich przypadków z pewnością jest wiele, pani przewodnicząca. Mówię o ludziach, którzy opuszczają armię, zdejmują mundury, stają się osobami cywilnymi i pracują na rzecz przemysłu – mam nadzieję – krajowego. Oczywiście, w resorcie obrony narodowej – jak powiedział pan mister Skrzypczak – obowiązują pewne reguły. Te reguły obowiązują nie tylko żołnierzy i pracowników wojska pracujących w resorcie, ale w ogóle wszystkich ludzi w Polsce. Mianowicie jest ustawa o ochronie informacji niejawnych…

Poseł Michał Jach (PiS):

Przepraszam, może zacznie pan jednak mówić bardziej do mikrofonu, bo trudno pana zrozumieć.

Dyrektor departamentu w MON Romuald Hoffmann:

Tak, że w tym przypadku nie unikniemy odejść. Nie unikniemy tego, że ktoś będzie postępował wbrew prawu. W związku z tym, jeżeli jest taka sytuacja, to należałoby ścigać ją na gruncie prawa. Natomiast chciałem tu zwrócić uwagę, że w resorcie obowiązuje decyzja ministra obrony narodowej dotycząca kontaktów z firmami zagranicznymi. Stąd z pewnością ten pan poszukuje kontaktów, chociaż może był to nasz kolega, który kiedyś z nami współpracował, że obowiązują nas regulacje wewnątrzresortowe dotyczące przeciwdziałania korupcji. W związku z tym tylko niektóre instytucje mogą się komunikować z przemysłem. Te reguły są jasno określone. Stąd prawdopodobnie ten pan poszukuje kontaktów, dlatego że wszyscy przestrzegamy tych regulacji.

Poseł Jadwiga Zakrzewska (PO):

A wojsko go wykształciło.

Dyrektor departamentu w MON Romuald Hoffmann:

Żyjemy w wolnym kraju. W związku z tym każdy ma prawo podejmować decyzje, które są związane z jego życiem.

Teraz przejdę do odpowiedzi na pytanie pana posła Kamińskiego. Oczywiście resort obrony narodowej to odczuł. Ja raczej nie nazywam tego atakami. To był protest. Tak chciałbym to odczytywać. Był to protest społeczeństwa w związku z chęcią wprowadzenia zapisów ACTA. Oczywiście, kiedy społeczeństwo pobudzone przez prasę, bo te rzeczy były publikowane, chciało skorzystać ze stron internetowych, siłą rzeczy stało się atakującym, gdyż obciążało łącza teleinformatyczne, czy telekomunikacyjne, które pozwalają na korzystanie z zasobów witryn internetowych resortu obrony narodowej. Zdarzały się również osoby nieprzyjazne, które wykorzystując tę sytuację chciały dokonać włamań. W związku z tym odnotowaliśmy również duże obciążenie serwerów, które obsługują strony internetowe. Takie obciążenie powoduje również to, że serwery odpowiadają z dużym opóźnieniem. Siłą rzeczy musieliśmy tutaj reagować na bieżąco. Chciałbym tutaj powiedzieć, że resort był chyba jedynym resortem, w którym funkcjonowały strony internetowe. Chociaż z opóźnieniem, jednak odpowiadały na zapytania ze strony internautów. I chciałem zwrócić uwagę, że nie były to strony statyczne. Były to strony w pełni interaktywne.

Oczywiście, w tym zakresie wyciągnęliśmy też wnioski, a mianowicie wnioski dotyczące struktury technicznej. Siłą rzeczy trzeba się uczyć, może nie na błędach, ale na sytuacjach, których sami nigdy byśmy sobie nie zasymulowali. W związku z tym zmieniona została również infrastruktura techniczna, ale nie w sensie bezpieczeństwa, nie w takim sensie, że tego nie było. Po prostu zostały zwiększone możliwości przetwarzania i separacji ruchu internetowego, jak i rozdzielenia tego ruchu na poszczególne inne serwery. Oczywiście, to również przekłada się na bezpieczeństwo, gdyż jednocześnie

dokonywaliśmy analizy sposobu prób włamania się do systemu. W związku z tym przekłada się to również na procedury operacyjne i sposób działania podległych mi służb. Jednocześnie pozwoliło to nam na dołączenie następnych przypadków, które mogliśmy zapisać w procedurach operacyjnych. Mogliśmy powiedzieć służbom, jak mają reagować w takich przypadkach.

Tak, że mogę powiedzieć, iż było to doświadczenie, które przetestowało system reagowania na incydenty komputerowe i pod względem technicznym i pod względem organizacyjnym. Muszę powiedzieć, że poziom był dobry. Zdefiniowany wcześniej decyzją ministra obrony narodowej system reagowania na incydenty komputerowe zadziałał. To taki wniosek, jeżeli chodzi o działania w styczniu 2012 r. Dziękuję.

Poseł Mariusz Antoni Kamiński (PiS):

A ataszaty?

Dyrektor departamentu w MON Romuald Hoffmann:

A, ataszaty, przepraszam bardzo. Jeśli chodzi o ataszaty, to w tej chwili również moi koledzy są w podróżach służbowych i realizują część inwestycji związanych z przyłączeniem ataszatów do infrastruktury telekomunikacyjnej resortu obrony narodowej. Chcę powiedzieć, że w przyszłości to raczej Ministerstwo Spraw Zagranicznych będzie prawdopodobnie korzystało z naszych zasobów, a nie my z zasobów Ministerstwa Spraw Zagranicznych. Oczywiście, do komunikacji z ataszatami wykorzystujemy wszystkie przynależne nam środki łączności, w tym również Internet i odpowiednie środki ochrony kryptograficznej, o których tutaj ze zrozumiałych względów nie wolno mi mówić. Nie mogę tego powiedzieć. Dziękuję bardzo.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Pan poseł Jach.

Poseł Michał Jach (PiS):

Dziękuję. Panie przewodniczący, panie ministrze, mam kilka uwag dotyczących tej informacji. Otrzymaliśmy tutaj informację, która – w moim przekonaniu – pokazuje przykładowy wzór, jak to powinno wyglądać. Z tej informacji nie wynika, na jakim etapie jesteśmy w tych poszczególnych sześciu punktach, jeśli chodzi o ich realizację, czy w ogóle ją zaczęliśmy, czy jest ona już blisko końca. To najbardziej zwróciło moją uwagę.

W pkt 2 jest mowa o budowie centrów przetwarzania informacji. Chciałbym usłyszeć kilka bardziej konkretnych informacji. Funkcjonowanie ilu docelowo takich centrów przewiduje resort? Ile z nich już funkcjonuje? Kiedy przewiduje się docelowe funkcjonowanie tych centrów? W końcowym fragmencie informacji jest zdanie, które niepokoi. Napisano, że konsolidacja serwerowni z duże centra pozwoli na uruchomienie. Czyli wygląda to tak, jak gdyby dopiero ktoś myślał o tym, żeby te serwerownie konsolidować.

W punkcie dotyczącym stosowania urządzeń kryptograficznych również nie jestem przekonany, że posiadamy tę kryptografię na miarę członka NATO i na miarę zapewnienia odpowiedniego bezpieczeństwa. Tutaj znowu jest takie zdanie. Te zdania wtrącają słuchacza w konfuzję. „W chwili obecnej resort obrony narodowej oczekuje na zakończenie procesu certyfikacji nowoczesnych urządzeń IP Crypto, które pozwolą…” itd. Chciałbym wiedzieć, jaka jest perspektywa czasowa. Mam również pytanie, czy przy zapewnieniu tych systemów kryptograficznych wykorzystuje się osiągnięcia polskiej nauki? Według wiedzy, jaką mam – jest to wiedza gazetowa – polska nauka posiada dość interesujące osiągnięcia w dziedzinie kryptografii.

Kolejne pytanie dotyczy standaryzacji wykorzystywanych narzędzi. Chwali się pan, że ostatnio zakupiono nowoczesne systemy. Posiadamy również dostęp do baz tej firmy. Oczywiście mówię o firmie Microsoft. Chciałbym wiedzieć, jak wygląda ta standaryzacja. Mamy Ministerstwo Administracji i Cyfryzacji. Chciałbym wiedzieć, czy ta standaryzacja dotyczy tylko standaryzacji wewnątrz resortu? Czy dotyczy również standaryzacji międzyresortowych? Wydaje się, że ministerstwo cyfryzacji zostało powołane po to, żeby to ujednolicić. Czy ta standaryzacja jest jakoś konsultowana? Czy ta standaryzacja obowiązuje we wszystkich resortach, z którymi resort obrony narodowej współpracuje?

Czy dopiero po zakupie tych narzędzi usiłuje się dostosować te narzędzia do współpracy z innymi resortami? Dziękuję.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Pani posłanka Sławiak.

Poseł Bożena Sławiak (PO):

Ja chciałam nawiązać do informacji w materiale dotyczącej współpracy z firmą Microsoft, która dostarcza oprogramowanie systemowe i biurowe na potrzeby systemów informatycznych przetwarzających informacje niejawne, na potrzeby resortu obrony narodowej. Czy są jakieś zabezpieczenia dotyczące możliwości skorzystania z tych informacji przez samą firmę Microsoft? Chodzi mi konkretnie o własne nakładki kryptograficzne. Czy są stosowane? Dziękuję.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Pan poseł Dorn.

Poseł Ludwik Dorn (SP):

Dziękuję bardzo. Ja mam następujące pytania. Jedno odnosi się do kwestii, którą zauważył pan poseł Jach. Nie bardzo wiemy, co jest stanem obecnym, jeśli chodzi o bezpieczeństwo teleinformatyczne, a co jest – może nie pobożnym życzeniem – ale w trakcie realizacji? Jakie są terminy realizacji? W związku z tym nie bardzo wiadomo, do czego odnosi się tak wysoka samoocena. Czy do tego, co już istnieje, czy do tego, co ma zaistnieć? Gdyby pan minister i jego współpracownicy zechcieli dokonać takiego rozróżnienia tego, co jest, od tego, co będzie, z zarysowaniem pewnego horyzontu czasowego, to bardzo by to nam pomogło.

Następne pytanie. Ja chciałbym dowiedzieć się czegoś bliższego o tym Narodowym Centrum Kryptologii. Co to w ogóle ma być? Jest ono tworzone wspólnie z Agencją Bezpieczeństwa Wewnętrznego. Czy to ma być wspólnie budowany organ centralny? Czy ma to być jednostka organizacyjna wewnątrz Ministerstwa Obrony Narodowej, czy sił zbrojnych? Czytamy też, że jeśli chodzi o Narodowe Centrum Kryptologii, to jego głównym zadaniem byłoby opracowanie algorytmu ochrony kryptograficznej, m.in. na potrzeby sił zbrojnych Rzeczypospolitej Polskiej. Ale na czyje jeszcze inne potrzeby poza siłami zbrojnymi Rzeczypospolitej Polskiej, skoro użyto tu określenia „m.in."? Czy w ogóle, jeśli chodzi o to Narodowe Centrum Kryptologii, to będzie ono potrzebowało umocowania ustawowego, bądź w niższym akcie prawa powszechnie obowiązującego, czy tylko wewnętrznego zarządzenia szefa resortu? No i jak to będzie z obsadą kadrową? Czy będzie ona mieszana – żołnierze, bądź pracownicy cywilni wojska i funkcjonariusze, bądź pracownicy cywilni Agencji Bezpieczeństwa Wewnętrznego? Na czym tutaj ma polegać ta wspólna praca z Agencją Bezpieczeństwa Wewnętrznego?

I pytanie trzecie. Też odnosi się do umowy z Microsoft podobnie, jak pytanie pani posłanki Sławiak. Czy to jest tak, że jeśli chodzi o oprogramowanie systemowe systemów przetwarzających informacje niejawne to w jakiejś mierze jesteśmy uzależnieni od szlaku? Inaczej mówiąc, jeżeli już raz wybrało się Microsoft, to powoduje może nie tyle konieczność, co pewną użyteczność – w ramach minimalizacji kosztów – podążania tym samym szlakiem. Żeby była jasność, to ja nie jestem fanatycznym przeciwnikiem Microsoftu i fanatycznym zwolennikiem np. Linuksa. Jaka jest w tym zakresie polityka, czy pogląd Ministerstwa Obrony Narodowej? Dziękuję.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Proszę uprzejmie. Kto odpowie? Pan dyrektor Hoffmann, tak? Proszę bardzo.

Dyrektor departamentu w MON Romuald Hoffmann:

Dziękuję. Panie przewodniczący, wysoka Komisjo, w sprawie budowy centrów przetwarzania informacji. Technologia postępuje i to bardzo, bardzo szybko. Jesteśmy zobowiązani do modernizacji już istniejących ośrodków lub do lokalizacji nowych centrów przetwarzania danych jako, że ilość danych, które są przetwarzane w resorcie obrony narodowej, ciągle wzrasta. Istniejące ośrodki obliczeniowe wymagały modernizacji. Stąd

też takie lokalizacje zostały zmodernizowane. W tej chwili mówię o Warszawie. Kończymy budowę, czy modernizację pozostałych ośrodków, których jest razem 9. Są one zlokalizowane w Warszawie, Bydgoszczy, Opolu, Szczecinie, Olsztynie, w Krakowie. To rozłożenie wynika przede wszystkim z już istniejącej infrastruktury, jak i z rozwiązań telekomunikacyjnych. Polska została podzielona na kilka obszarów, jeżeli chodzi o możliwości przetwarzania informacji, w związku z czym takie lokalizacje zostały wybrane na modernizację, jak i na nowe inwestycje.

To nie oznacza, że proces, o którym tutaj mówimy będzie miał jakiś koniec. Jest to proces, który został podzielony na poszczególne etapy. W związku z tym myślę, że po jakimś okresie funkcjonowania istniejących ośrodków, które zostały zmodernizowane, będzie musiała następować modernizacja w wyniku postępu technologicznego. Siłą rzeczy za kilka lat zostanie ona wymuszona przez potrzeby informacyjne i informatyczne resortu obrony narodowej. Jednocześnie pojawiły się nowoczesne technologie, które pozwalają w niezawodny sposób organizować i łączyć ośrodki przetwarzania po to, żeby było przetwarzanie rozproszone. Zatem te technologie wymuszają również odpowiednią modernizację tych serwerowni. Oznacza to, że te serwerownie, które był do tej pory, były niewystarczające, a wdrażanie coraz nowszych systemów informatycznych, chociażby w obszarze logistyki, kadr i finansów, wymaga coraz większych mocy obliczeniowych.

Co więcej, bezpieczeństwo teleinformatyczne jest zapewniane też przez oprogramowanie. Ono też wymaga odpowiedniej infrastruktury. Wymaga mocy obliczeniowych. Siłą rzeczy, takie inwestycje będą musiały być czynione co pewien czas. Inwestycje są ujmowane w programie modernizacji technicznej. Są realizowane w cyklach inwestycyjnych, zgodnie z Prawem budowlanym. Oprócz serwerowni stacjonarnych przewidujemy również pozyskanie w przyszłości tzw. serwerowni kontenerowych, które mogłyby zostać wykorzystane w przypadku potrzeby przeniesienia serwerowni już istniejących, albo wyłączenia ich z eksploatacji. Wymaga to przede wszystkim odpowiednich inwestycji i rozwiązań oraz wyboru odpowiednich technologii.

Natomiast odnosząc się do kryptografii chcę zwrócić uwagę, że obowiązuje nas ustawa o ochronie informacji niejawnych. Wojsko jest zobowiązane do używania urządzeń certyfikowanych przez służby – przez Służbę Kontrwywiadu Wojskowego lub przez Agencję Bezpieczeństwa Wewnętrznego. Tylko takie urządzenia możemy wykorzystywać. Sformułowanie, że oczekujemy na zakończenie certyfikacji, jest zgodne z prawdą. Zgodnie z planami Służba Kontrwywiadu Wojskowego powinna zakończyć certyfikację niektórych urządzeń jeszcze w tym roku. Potem nastąpi proces pozyskiwania tych urządzeń. Co więcej, są to urządzenia budowane z wykorzystaniem polskiej kryptografii. Nie oznacza to, że w kraju jest tylko jeden ośrodek, który potrafi budować algorytm kryptograficzny i rozwiązania techniczne, elektroniczne rozwiązania kryptograficzne. Zatem kryptografia, którą stosujemy, jest w pełni kryptografią polską, a jednocześnie wykorzystuje w pełni doświadczenia naszego potencjału naukowego.

Odnosząc się do standaryzacji, a tu odnoszę się też do firmy Microsoft, chcę zwrócić uwagę, że historia pokazuje, iż również resort obrony narodowej, jak i całe społeczeństwo w Polsce wykorzystują tę technologię. Jest to pewna zaszłość historyczna. Jest to związane z pewnymi inwestycjami i ochroną inwestycji, które wcześniej zostały poczynione. Inwestujemy w tę technologię. Związane to jest nie tylko z zakupem licencji i wsparcia technicznego, ale również ze szkoleniem użytkowników. A szkolenie, czy nauczenie użytkowników wykorzystania innych technologii, jeżeli mówimy o użytkowniku końcowym, też kosztuje. To też liczymy. Firma Microsoft nie ma dostępu do naszych zasobów. Chciałem na to zwrócić uwagę. Wszystkie rzeczy, które realizujemy w ramach naszych sieci, jest realizowane siłami resortu obrony narodowej. Są to zarówno informatycy wojskowi, jak i informatycy cywilni. W związku z tym nie ma tutaj mowy o dostępie firmy Microsoft do naszych zasobów. Takiego przypadku do tej pory nie było i raczej go nie będzie. Wynika to przede wszystkim z tego, że resort obrony narodowej przywiązuje szczególną wagę do bezpieczeństwa informacji. Stąd prowadzimy taką politykę.

Ale nie oznacza to, że wykorzystujemy tylko oprogramowanie firmy Microsoft. A mianowicie wykorzystujemy i zakupujemy też oprogramowanie innych producentów.

Wynika to z faktu, że nie tylko oprogramowanie Microsoftu jest używane w resorcie. Oprogramowanie innych producentów jest stosowane również w zautomatyzowanych systemach dowodzenia. Stąd też trzeba to oprogramowanie kupować. Ale nie uciekamy również od open source, czyli od oprogramowania otwartego. Niedawno resort obrony narodowej zamknął przetarg na zakup wsparcia do oprogramowania open source, które pozwoli nam wykorzystywać te programy w sieci Internet. Wynika to przede wszystkim z tego, że tego oprogramowania jest bardzo dużo. Jednocześnie to wsparcie jest związane przede wszystkim z przeszkoleniem zasobów osobowych, które mamy w resorcie obrony narodowej. To też wymaga wykształcenia wysoko wykwalifikowanych ludzi w tym zakresie. Zatem oprogramowanie open source nie jest tak do końca tanie. Ono nie jest bezpłatne. Można byłoby tak kolokwialnie powiedzieć, dlatego że my też musimy ponieść pewien wysiłek, żeby zbudować zespoły, które to oprogramowanie będą utrzymywać, rozwijać i jednocześnie użytkować. Mówię tu o oprogramowaniu, które będzie służyło przede wszystkim do zbudowania wydajnych systemów poczty elektronicznej w sieci InterMON.

Stosujemy również, realizujemy również standaryzację sprzętu. Ale ta standaryzacja wynika z tego faktu, że przez wiele lat w procesie pozyskiwania resort obrony narodowej pozyskiwał sprzęt o różnej jakości. W związku z tym ten sprzęt, który chcemy zakupić, standaryzujemy co do jakości. Publikujemy tzw. standardy informatyki, które służą nam do tego, żebyśmy wewnątrz resortu mogli planować również przyszłościowe potrzeby w resorcie obrony narodowej. Chcę zwrócić uwagę, że czas życia komputera, bo komputer zużywa się, to okres 5 lat. Amortyzacja komputera następuje po 5 latach. Siłą rzeczy musi nastąpić odtworzenie zasobów, które posiadamy w resorcie obrony narodowej. Dla stacji roboczych jest to 5 lat, a dla serwerów jest to od 7 do 8 lat. Łatwo policzyć, zaczynając do 2008 r., że już w tym roku powinniśmy zacząć wymieniać sprzęt komputerowy, który znajduje się na stanowiskach pracy. Wynika to z tego, że oprogramowanie, które wdrażamy w resorcie obrony narodowej, naszych systemów informatycznych wymaga coraz większych mocy obliczeniowych.

Zatem komputery, które zostały nabyte 5 lat temu, już takiej mocy nie posiadają. W związku z tym jest to proces ciągły. Dotyczy to także serwerów, które są lokowane w poszczególnych serwerowniach. Jest to związane ze zwiększeniem ich mocy obliczeniowej, a również z zapotrzebowaniem na zasilanie. Zatem musimy też rozbudowywać dowiązania energetyczne, aby można było zaspokoić potrzeby. Przejdźmy do horyzontu czasowego. Jeżeli chodzi o system telekomunikacyjny, czyli gdy mówimy o transmisji telekomunikacyjnej, to resort obrony narodowej ma zawarte umowy telekomunikacyjne z operatorami. Są one odnawiane co pewien czas. Wraz ze wzrostem zapotrzebowania na transmisje, a jednocześnie wraz z nowymi rozwiązaniami technicznymi w obszarze telekomunikacji u dostawców, te umowy co jakiś czas muszą być renegocjowane. Jest to w cyklu ok. pięcioletnim.

Narodowe Centrum Kryptologii będzie – takie są założenia, gdyż w tej chwili trwają w resorcie obrony narodowej dyskusje na ten temat – instytucją wewnątrzresortową. W trakcie dyskusji jest zarządzenie ministra obrony narodowej powołujące ten ośrodek, który ma zająć się potrzebami kryptograficznymi resortu obrony narodowej. Ale tu uwaga. Resor obrony narodowej jest oczywiście największym konsumentem rozwiązań kryptograficznych. Niemniej jednak uważamy, że resort może się podzielić tymi rozwiązaniami na rzecz instytucji rządowych. Dlaczego? Dlatego, że przewidujemy, iż w przyszłości nasze systemy informatyczne, które są systemami niejawnymi, mogą się również łączyć z systemami rządowymi. Musimy się do tego przygotować. Zatem będzie to organizacja, która będzie wspierać kryptografię w resorcie obrony narodowej. Będzie to instytucja wewnętrzna.

Współpracujemy z Agencją Bezpieczeństwa Wewnętrznego z prostej przyczyny. Jest to krajowa władza bezpieczeństwa. W związku z tym wszelkie rozwiązania kryptograficzne muszą być z Agencją Bezpieczeństwa Wewnętrznego dyskutowane. Jednocześnie, w związku z prowadzeniem polityki kryptograficznej przez Agencję Bezpieczeństwa Wewnętrznego musimy omówić, czy przedyskutować projekty związane z algorytmami kryptograficznymi. Przy tej okazji chciałbym powiedzieć, że te rozwiązania, które zostały zaproponowane przez polską

naukę, mogą znaleźć zastosowanie w resorcie obrony narodowej pod jednym warunkiem – że przejdą w sumie niełatwy proces certyfikacji w Agencji Bezpieczeństwa Wewnętrznego lub w Służbie Kontrwywiadu Wojskowego. Chciałbym tutaj wspomnieć, że możemy stosować i stosujemy rozwiązania, które są certyfikowane przez jedną, albo drugą służbę. Jest to zgodne z ustawą o ochronie informacji niejawnych.

Domyślam się, że z braku czasu nie w pełni wyczerpię ten temat. Jednak przy Narodowym Centrum Kryptografii chciałbym powiedzieć, że obsada będzie oczywiście wypracowana w trakcie dalszych dyskusji w resorcie obrony narodowej dotyczących typów specjalistów, którzy powinni znaleźć tam swoje miejsce. Domyślam się, że będą to zarówno żołnierze, naukowcy wojskowi w mundurach, jak i pracownicy cywilni, a – co więcej – ośrodek ten będzie otwarty również na naukę polską w celu współpracy. Mam nadzieję, że wyczerpałem wszystkie odpowiedzi.

Przewodniczący poseł Stefan Niesiołowski (PO):

Aż za bardzo. Dziękuję bardzo. Prosiłbym pana o zwięzłość wypowiedzi w przyszłości.

Dyrektor departamentu w MON Romuald Hoffmann:

Tak jest, panie przewodniczący.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo.

Proponuję przejście do drugiego punktu, tj. do informacji ministra obrony narodowej na temat uwzględnienia potrzeb obronności w planowaniu i zagospodarowaniu przestrzennym kraju. Pani minister Oczkowicz. Proszę bardzo.

Podsekretarz stanu w MON Beata Oczkowicz:

Panie przewodniczący, szanowna Komisjo, celem mojego wystąpienia jest zaprezentowanie aktualnych problemów występujących w obszarze zapewnienia bezpieczeństwa państwa poprzez uwzględnienie potrzeb obronności w planowaniu i zagospodarowaniu przestrzennym kraju. Są to problemy wynikające z aktualnego stanu prawnego – z obowiązującej ustawy z 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym oraz z rozporządzenia ministra infrastruktury w sprawie sposobu uwzględnienia w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa z 7 maja 2004 r. Dodam, że to rozporządzenie zawiera wyłącznie wiele ogólnych zapisów, które powtarzają ustalenia zawarte w ustawie. Tym samym nie wnosi ono żadnych szczegółowych przepisów, które mogłyby ułatwić wykonywanie zadań organom wojskowym.

Chciałabym również wskazać potrzebę zwiększenia roli organów rządowych kosztem ograniczenia zbyt znaczącej – według Ministerstwa – roli samorządów lokalnych, od których obecnie zależy sprawne i skuteczne wprowadzanie w życie potrzeb obronnych dotyczących obszaru planowania i zagospodarowania przestrzennego, m.in. przez podjęcie uchwały w sprawie przystąpienia do opracowania planu zagospodarowania przestrzennego, a także przyjęcia planów miejscowych. Mając na uwadze aktualny stan prawny chcę stwierdzić, że istniejące regulacje prawne w obszarze uwzględniania potrzeb obronnych w planowaniu i zagospodarowaniu przestrzennym są niewystarczające z punktu widzenia zabezpieczenia potrzeb obronności państwa, czego przykładem mogą być występujące problemy z ustalaniem i utrzymaniem stref ochronnych terenów zamkniętych.

Coraz częściej występują problemy z właściwym funkcjonowaniem obiektów i kompleksów wojskowych, w wyniku zacieśniania się wokół nich tzw. pętli urbanistycznych, które są wynikiem ekspansji inwestycji na danym terenie. Urzędy nie mają opracowanych planów miejscowych, a tym samym wydają indywidualne decyzje lokalizacyjne i indywidualne pozwolenia na budowę. Potrzeby obronne związane z nakładaniem na właścicieli terenów wokół obiektów i kompleksów wojskowych ograniczeń zagospodarowania i użytkowania tych terenów postrzegane są przez miejscową, lokalną ludność, jako bariera w rozwoju regionu. Stąd też dążenie samorządu do zmniejszenia tych ograniczeń m.in. przez wystąpienia o zmniejszenie, bądź zniesienie stref ochronnych terenów zamkniętych, a także utrudnianie wprowadzania takich potrzeb do planów miejscowych. Z uwagi na istniejące potrzeby obronne oraz występujące poważne problemy,

szczególnego usprawnienia wymaga procedura ustalania stref ochronnych wojskowych terenów zamkniętych i wzrastająca rola organów administracji rządowej – wojewody – w tym, działaniu. Wskazane wydaje się, żeby uniezależnić wprowadzanie tych potrzeb obronnych od rozstrzygnięć samorządu lokalnego.

Szanowna Komisjo, po okresie doświadczeń związanych z funkcjonowaniem ustawy z 2003 r. o planowaniu i zagospodarowaniu przestrzennym w zakresie dotyczącym ujmowania w planach miejscowych potrzeb obronnych, resort obrony narodowej wnosił przy kilku sposobnościach wiele propozycji, niestety, z różnym skutkiem, dotyczących nowelizacji tego aktu prawnego. Kiedy na przełomie lat 2009-2010 prowadzone były prace nad istotną nowelizacją powyższej ustawy, resort w wyniku zebranych doświadczeń podjął się zadania generalnego uporządkowania problematyki uwzględniania potrzeb obronnych i przedstawił kompleksowe propozycje nowelizacji zapisów ustawy dotyczących tego problemu. Efektem tych starań było zobowiązanie ówczesnego ministra infrastruktury do współpracy w powyższym zakresie w kolejnych pracach legislacyjnych nad ustawą. Wskazał on propozycję zawarcia tych regulacji w odrębnej ustawie. Jednak do takiej sytuacji nie doszło.

W 2009 r., w związku z przewidywanym przystąpieniem ministra infrastruktury, obecnie ministra transportu, budownictwa i gospodarki morskiej, do nowelizacji rozporządzenia w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa, resort przedstawił również katalog zagadnień proponowanych do uwzględnienia w projekcie nowego rozporządzenia. Jednak te prace zostały zawieszone przez Ministerstwo Infrastruktury.

Szanowna Komisjo, w ocenie resortu obecnie samorządy zbyt znacząco decydują o uwzględnianiu potrzeb obronnych, ponieważ to od ich uchwał w sprawach zagospodarowania przestrzennego faktycznie zależy prawne wprowadzenie w życie naszych potrzeb. Istniejące procedury dyscyplinujące władze samorządowe ze strony wojewody, m.in. z uwagi na ich przewlekłość – niestety – nie sprawdzają się. W konsekwencji do czasu uchwalenia planu gmina może kształtować przestrzeń wokół naszych terenów w sposób nie zawsze zgodny z potrzebami obronnymi. Dodam, że w poprzedniej regulacji prawnej wojewoda, jako organ administracji rządowej, ustalał strefy ochronne dla terenów zamkniętych. Ustalał to w formie decyzji administracyjnej. Takie rozwiązanie było zdecydowanie bardziej zasadne.

Panie przewodniczący, szanowna Komisjo, Ministerstwo rozpoczęło działania legislacyjne zmierzające do usprawnienia procedur związanych z uwzględnieniach potrzeb obronnych w dokumentach dotyczących właśnie tego obszaru. Ja występuję z wnioskiem o wsparcie działań resortu obrony narodowej, działań mających na celu podjęcie prac legislacyjnych przez ministra transportu, budownictwa i gospodarki morskiej w zakresie nowelizacji rozporządzenia w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa celem wyeliminowania obecnie występujących problemów. To wszystko z mojej strony.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję pani minister. Otwieram dyskusję. Proszę uprzejmie. Pan poseł Budnik.

Poseł Jerzy Budnik (PO):

Dziękuję bardzo. Pani minister, ja miałem nadzieję na to, że inicjatywa wyjdzie z Ministerstwa Obrony Narodowej, oczywiście w konsultacji z Ministerstwem Infrastruktury. Pani prosi nas o pomoc. My możemy podjąć inicjatywę komisyjną, ale byłoby to bez sensu, jeżeli miałby nad tym pracować resort infrastruktury. Może nam pani to przybliży. Czy przesłaliście już jakieś rekomendacje do Ministerstwa i prosicie nas, żebyśmy to poparli, kiedy będzie to procedowane w Sejmie? Na jakim etapie jesteście z tymi zmianami? Oczywiście, one są istotne. Ja widzę, że nastąpiło tutaj takie przegięcie. Kiedyś było odwrotnie. Kiedyś to wojsko prawie blokowało rozwój miast.

Mówię tu o swoim terenie. Wiadomo, że np. półwysep Helski był prawie zablokowany, czy Oksywie. Dopiero teraz je wyłączyliśmy, uchylając jeszcze przedwojenny dekret o ustanowieniu rejonu umocnionego. Teraz widzę, że jest odwrotnie. To samorządy uniemożliwiają wam rozbudowę niektórych kompleksów wojskowych, szczególnie tych, które

są objęte jakimiś utajnionymi regulacjami. Wracam do swojego pytania. Pani minister, czy w tej chwili już współpracujecie? Czy wysłaliście tam swoje rekomendacje, czy czekacie, aż my to zrobimy?

Przewodniczący poseł Stefan Niesiołowski (PO):

Jeszcze pan poseł, sekundkę pani minister. Mamy taki zwyczaj, że 3 osoby zadają pytania, a potem jest łączna odpowiedź. Pan poseł Dorn.

Poseł Ludwik Dorn (SP):

Pani minister, to jest tak, że to nie jest tylko bolączka resortu. Wiadomo, że do czasu uchwalenia planu jest o wiele większa dowolność. W związku z tym tych planów jak nie było, tak nie ma. Prawda? Nic się tutaj nie zmienia. Nikt nie chce sobie nakładać kagańca, prawda? No, ale to jest jakby zasadniczy błąd w samej ustawie, która prowokuje taki mechanizm. Tutaj tego nie zmienimy.

Moje pytanie jest takie. Co oznacza to poproszenie o wsparcie? Tak, jak panią minister zrozumiałem, to rzecz polega nie na nowelizacji ustawy, ale na nowelizacji rozporządzenia tylko, że minister właściwy do tego rozporządzenia zaparł się i nie chce. Czyli nie możecie się dogadać w rządzie. Tak, że o co resortowi tak konkretnie chodzi? Żebyśmy wydali opinię, że dobrze byłoby, aby i żeby pan minister właściwy do spraw transportu coś zrobił? Tak kawę na ławę.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo panu posłowi. Jeżeli nie ma już głosów, to zamykam dyskusję, oczywiście wstępnie. Pani minister Oczkowicz. Proszę bardzo.

Podsekretarz stanu w MON Beata Oczkowicz:

Tak, jak powiedziałam, my zgłosiliśmy swoje uwagi do rozporządzenia, które miało być nowelizowane. Jednakże prace nad tym rozporządzeniem zostały wstrzymane przez Ministerstwo. My pod koniec 2012 r., czyli praktycznie całkiem niedawno wróciliśmy do tematu. Ja oczekiwałabym wsparcia, tak naprawdę każdego z pań i panów posłów, żeby to rozporządzenie weszło w życie. Oczywiście to, co przygotujemy, będzie tutaj przedstawione. Tak, że chodzi bardziej o takie wsparcie poselskie.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Jeżeli nie ma uwag, to zanim przejdziemy do spraw bieżących – jeżeli będą – stanowisko do pierwszego punktu chciała zaproponować pani przewodnicząca Zakrzewska. Proszę bardzo.

Poseł Jadwiga Zakrzewska (PO):

Dziękuję. „Należy podkreślić, że nadal istnieje potrzeba wypracowania na poziomie państwowym jednolitego systemu gwarantującego sprawną reakcję służb państwowych, w tym wojska i ich podmiotów, na poważne incydenty komputerowe oraz koordynację działań w sytuacji kryzysowej państwa.”.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dziękuję bardzo. Czy są uwagi? Proszę bardzo. Pan poseł Dorn.

Poseł Ludwik Dorn (SP):

No, ale co to jest? Projekt opinii? Czy co?

Poseł Jadwiga Zakrzewska (PO):

Nie. Konkluzja z dzisiejszej dyskusji.

Poseł Ludwik Dorn (SP):

Znaczy, regulamin nie przewiduje konkluzji. Może być opinia, dezyderat, stanowisko. No, tak bardziej regulaminowo.

Przewodniczący poseł Stefan Niesiołowski (PO):

Opinia, panie pośle.

Poseł Ludwik Dorn (SP):

Opinia, tak?

Przewodniczący poseł Stefan Niesiołowski (PO):

Tak.

Poseł Ludwik Dorn (SP):

Ja nie jestem przeciw temu, co proponuje pani przewodnicząca Zakrzewska, tylko chciałbym, żeby to było regulaminowo.

Przewodniczący poseł Stefan Niesiołowski (PO):

Odpowiadam panie pośle. Opinia, tak opinia.

Poseł Ludwik Dorn (SP):

Ale pan tutaj mówi, że opinia musi być do kogoś skierowana.

Przewodniczący poseł Stefan Niesiołowski (PO):

Co pani proponuje? Do ministra odpowiada pani?

Poseł Jadwiga Zakrzewska (PO):

Raczej do premiera, ponieważ chodzi tu o sprawy na poziomie państwowym. Chodzi o koordynację działań wszystkich służb.

Przewodniczący poseł Stefan Niesiołowski (PO):

Panie pośle Dorn, czy możemy się zgodzić na konsensus i przyjąć to, co zaproponowała pani Zakrzewska?

Poseł Ludwik Dorn (SP):

Tak. Czy pani przewodnicząca jeszcze raz byłaby uprzejma?

Poseł Jadwiga Zakrzewska (PO):

„Należy podkreślić, że nadal istnieje potrzeba wypracowania na poziomie państwowym jednolitego systemu gwarantującego sprawną reakcję służb państwowych, w tym wojska i ich podmiotów, na poważne incydenty komputerowe oraz koordynację działań w sytuacji kryzysowej państwa.”.

Poseł Ludwik Dorn (SP):

Przepraszam bardzo, ale czy to jest taka konkluzja, wniosek, stanowisko opracowane pod wpływem przedstawionych informacji, bo ja w tych informacjach nie odnotowałem stwierdzenia takiego faktu, że to, co pani przewodnicząca postuluje, nie istnieje? Raczej były tam pewne elementy pozytywnej oceny obecnego stanu rzeczy, prawda? A tutaj mamy do czynienia, znaczy przesłanką tej opinii jest to, że coś w obecnym stanie rzeczy niedomaga, skoro nadal istnieje potrzeba. W związku z tym mam pytanie. Czy rzeczywiście coś tak niedomaga, że nadal istnieje potrzeba?

Przewodniczący poseł Stefan Niesiołowski (PO):

Panie pośle, mogę tylko rozwiać pana wątpliwości regulaminowe. Jeżeli pan jest przeciw, to ja nie chcę głosować. Jeżeli nie ma konsensusu, to ja wycofam tę opinię i nie będziemy dyskutować. Zgodnie z regulaminem, art. 160 mówi, że do ministra obrony możemy taką opinię skierować. Czy jest w tej sprawie konsensus w Komisji?

Poseł Waldemar Andzel (PiS):

Nie ma.

Przewodniczący poseł Stefan Niesiołowski (PO):

Jeżeli nie ma… Nie ma, tak?

Poseł Waldemar Andzel (PiS):

Nie ma.

Przewodniczący poseł Stefan Niesiołowski (PO):

Dobrze. Wycofujemy w takim razie. Dziękuję bardzo.

Jeszcze sprawy bieżące. Czy ktoś w sprawach bieżących?

Dziękuję bardzo. Zamykam powiedzenie Komisji.